POLICY 9.00 PHYSICAL ACCESS

Physical access to information resource assets and infrastructure will be restricted to those individuals who have a business need.

PURPOSE:

To minimize the likelihood that information technology resources and associated component integrity could be compromised.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure physical access to the information resources and infrastructure is restricted.
2. Ensure individual access privileges to tangible information technology resources reflect the individual's responsibilities for the resource object.
3. Protect critical state information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction.
4. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope includes the physical access to all State of Tennessee information technology resources and infrastructure.

Office for Information Resources (OIR)

1. Develop standards and guidelines for physical access to the information resource assets and infrastructure.
2. Ensure appropriate protective mechanisms are installed to restrict access to the information resource infrastructure, in coordination with appropriate departments.

Agency

1. Implement practices and procedures to ensure locally managed assets, such as workstations, are protected from unauthorized access.
2. Install protective mechanisms to restrict access to the local information resource infrastructure.
3. Limit physical access to authorized areas.
4. Ensure physical access is monitored and exceptions reported.

Individual Users/Clients

1. Limit physical access to authorized areas.
2. Refrain from behaviors that could compromise the physical protection of information technology resources.